UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/936,131	09/04/2001	Boris Balacheff	B-4295CT 619055-2	9453

22879 7590 08/01/2005

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 08/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/936,131	BALACHEFF ET AL.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38 and 41-61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,9-38 and 41-61* is/are rejected.

7)☒ Claim(s) *6-8* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *06/20/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

5.00

Response to Arguments

1. This communication is in response to applicants' response received on June 20, 2005.

2. Amendments of the specification and claims 21 and 27 are acknowledged.

3. Applicant's arguments have been fully considered but they are not persuasive.

4. With regards to independent claims 1, 25, 32, 38, 42 and 43, on pages 22, 25-29, applicants present similar arguments such as: "Applicants respectfully disagree with the Examiner's conclusion because there is no network mentioned anywhere in Lee, and thus the skilled person perusing Lee would have no motivation whatsoever to look at a reference directed to network reliability such as Sprurnk."

On the contrary, there are several indications in Lee that the invention is implemented in a distributed computing system (i.e., a computer network) (see, for example, col. 1, lines 10-14; col. 1, lines 25-31; col. 4, lines 41-47; col. 5, lines 17-24; col. 8, lines 53-57). Therefore, a person skilled in the art can be motivated to implement the teaching of Sprunk for checking the integrity of a network member by another network member (i.e., a component in the network) in the system of Lee.

5. On page 22, lines 21-25 of the remarks, applicants argue that: "In particular, Applicants disagree that Lee discloses, at the very least, the claimed token device that operates to make an integrity challenge to the monitoring component and that will not

undertake specific actions of which it is capable unless it receives a satisfactory response to the integrity challenge." And on page 23, lines 21-23, applicants argue that: "Lee does not teach, mention or hint anywhere that the card will not undertake specific actions unless it receives a satisfactory response to an integrity challenge."

In response to above, Lee discloses that when a smart card and a computing system authenticate each other (see, for example, col. 3, lines 60-67 and col. 6, lines 60-67) operations such as financial transaction, data transmission and application program execution (see col. 2, lines 40-48, col. 3, lines 32-40 and col. 8, lines 35-60) could be performed that otherwise in the case of an unsatisfactory response (i.e. unauthenticated card or system) would not happen. However, each of the mentioned operations is a specific action.

6. On page 24, lines 28-29 of the remarks, applicants argue that: "Applicants discern no teaching in this passage, nor anywhere else in Lee, of the host computer displaying verification data verifying correct operation of the computer..."

In response to above argument, the "... system 100 prompts the user to enter a PIN...", the "... the system 100 determines that the user is authorized and allows the user to gain entry into system 100", and the "... then the system 100 determines that the user is not authorized ..." in col. 17, lines 52-61 in Lee are indications of visual display of information on a monitor screen to a person of ordinary skill in the art. Furthermore, the use of a display screen in Lee is disclosed in col. 5, lines 50-53 and col. 5, lines 61-64.

7. In light of the above submission the previous rejection of claims is maintained.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claim 35 recites the limitation "said integrity response" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1, 2, 10-32, 38 and 41-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee (5,923,759) in view of Sprunk (5,822,431).

Claims 1 and 48

Lee discloses:

A system of computing apparatus comprising (Fig. 1):

a computing platform having a first data processor and a first data storage means (col. 5, lines 55-67);

a monitoring component having a second data processor and a second data storage means (col. 3, lines 43-67, where security module corresponds to the recited monitoring component); and

a token device being physically distinct and separable from said computing platform and said monitoring component (col. 6, lines 15-25),

wherein in one mode of operation, said token device operates to make an integrity challenge to said monitoring component and said token device will not undertake specific actions of which it is capable unless it receives a satisfactory response to said integrity challenge (col. 6, lines 52-67).

However, Lee does not expressly disclose that said monitoring component is configured to perform a plurality of data checks on said computing platform.

Sprunk teaches a mechanism that by which the integrity of a computing component is checked (corresponding to the recited a plurality of data checks) by another computing component (corresponding to the recited monitoring component) in order to find out the status of the first computing component (col. 1, lines 58-62; col. 3, lines 20-25; col. 5, lines 13-20; col. 6, lines 13-22; col. 13, lines 11-19).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Lee by the teaching of Sprunk, because it ensures that the network meets a minimum reliability standard (col. 8, lines 33-47).

Claims 2 and 49

Lee discloses:

token device receives a detailed response to said integrity challenge, and processes said integrity response to interpret said integrity response (col. 7, lines 17-34).

Claims 10 and 50

Lee discloses:

token device is requested to take an action (col. 6, lines 37-52).

Claims 11 and 51

Lee discloses:

token device requests to take an action (col. 6, lines 53-267).

Claim 12

Lee discloses:

The system as claimed in claim 1 in which said token device sends image data to said computer platform if a said satisfactory response to said integrity challenge is received, and said computer platform displays said image data (col. 7, lines 52-61, where prompting corresponds to displaying and entering PIN by the user corresponds to sending image).

Claims 13 and 52

Lee discloses:

The monitoring component is capable of establishing an identity of itself (col. 7, lines 17-25, where MAC corresponds to the recited identity).

Claims 14, 53 and 58

Lee discloses:

The system as claimed in claim 1, further comprising an interface means for interfacing between said monitoring component and said token device (col. 2, lines 59-65; col. 3, lines 3-41, col. 4, lines 53-64; col. 6, lines 15-25).

Claim 15 and 54

Lee in view of Sprunk discloses:

The system as claimed in claim 1, wherein said system of computing apparatus is configured such that said monitoring component reports said data checks to said token device as stated above for the like elements of claims 1 and 2, said data checks containing data describing a status of said computer platform (Sprunk, col. 3, lines 20-25; col. 6, lines 13-22).

Claim 16

Lee discloses:

The system as claimed in claim 1, wherein a said specific action comprises authorizing said computing platform to undertake a transaction on behalf of a user of said system (col. 1, lines 35-52; col. 8, lines 35-48).

Claim 17

This claim is rejected as applied to the like elements of claim 1 as stated above and further the following:

Lee discloses:

token device sends an integrity challenge to said monitoring component (col. 6, lines 53-65);

said monitoring component generates a response to said integrity challenge (col. 6, lines 53-65);

if said token device receives a satisfactory response to said integrity challenge, then said token device sends verification data to said computer platform, said verification data verifying correct operation of said computer platform (col. 6, lines 53-65; col. 7, lines 17-34); and

said computer platform displays said verification data on a visual display screen (col. 7, lines 52-61).

Claim 18

This claim is rejected as applied to the like elements of claims 1, 13, 14 and 15 as stated above.

Claim 19

This claim is rejected as applied to the like elements of claims 1, 14 and 15 as stated above.

Claim 20

Lee discloses:

The computing entity as claimed in claim 18, wherein said interface means is resident substantially wholly within said monitoring component (see Figs. 1 and 4). Fig. 1 of the application shows that the card reader 12 is not included in the monitoring component of 24.

Claim 21

Lee discloses:

The computing entity as claimed in claim 18, wherein said interface means is comprised by said computer platform (see Figs. 1, where system 100 comprises host processor and the).

Claim 22

Lee discloses:

The computing entity as claimed in claim 18, wherein said interface means comprises a PCSC stack in accordance with PCSC Workgroup PC/SC Specification 1.0 (col. 8, lines 22-34; col. 9, lines 14-36. where ISO layer corresponds to the recited PCSC stack. The PC/SC Specification 1.0 is a part of ISO specifications).

Claim 23

Lee in view of Sprunk discloses:

The computing entity as claimed in claim 18, wherein said monitoring component comprises a verification means configured to obtain a certification data independently certifying said status data, and to provide said certification data to said interface means (Lee, col. 7, line 62-col. 8, line 6; col. 9, lines 14-20, where the block of data corresponds to the recited status data that is the integrity information received from the computing platform as stated above in the case of claims 1 and 18).

Claim 24

Lee discloses:

The computing entity as claimed in claim 18, wherein said interface means is configured to send and receive data according to a pro-active protocol (col. 9, lines 14-32).

Claim 25

Lee discloses:

A method of obtaining verification of a state of a computer entity (col. 6, lines 53-60), said computer entity comprising a computer platform comprising a first data processor and a first memory means (col. 5, lines 55-67), and a monitoring component comprising a second data processor and a second memory means (col. 3, lines 43-67,

where security module corresponds to the recited monitoring component), said method comprising the steps of:

receiving an interrogation request signal via an interface of said computing entity (col. 6, lines 53-67); and

said monitoring component reporting a result message to said interface (col. 6, lines 53-67).

Lee, however, does not expressly disclose that said monitoring component performing a monitoring operation of said computer platform in response to a said received interrogation request signal and said result message describing a result of said monitoring operation.

Sprunk teaches a mechanism that by which the integrity of a computing component is checked (corresponding to the recited a monitoring operation) by another computing component (corresponding to the recited monitoring component) in order to find out or describe the status of the first computing component (col. 1, lines 58-62; col. 3, lines 20-25; col. 5, lines 13-20; col. 6, lines 13-22; col. 13, lines 11-19).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Lee by the teaching of Sprunk, because it ensures that the network meets a minimum reliability standard (col. 8, lines 33-47).

Claim 26

Lee discloses:

A method as claimed in claim 25, in which said monitoring operation comprises the steps of:

said monitoring component being able to report a set of certified reference data (Lee, col. 7, line 62-col. 8, line 6; col. 9, lines 14-20, where the block of data corresponds to the recited certified reference data); and

Lee, however, does not expressly disclose that said monitoring component carrying out one or a plurality of data checks on components of said computing platform and report the result of the data check.

Sprunk teaches a technique that by which the integrity of a computing component is checked (corresponding to the recited one or a plurality of data checks) by another computing component (corresponding to the recited monitoring component) in order to find out the status of the first computing component (col. 1, lines 58-62; col. 3, lines 20-25; col. 5, lines 13-20; col. 6, lines 13-22; col. 13, lines 11-19).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Lee by the teaching of Sprunk, because it ensures that the network meets a minimum reliability standard (col. 8, lines 33-47).

Claim 27

Sprunk discloses:

The method as claimed in claim 26, wherein said certified reference data includes a set of metrics to be expected when measuring particular components of said

computing platform, and includes digital signature data identifying an entity that certifies said reference data (col. 8, lines 33-47 and col. 10, lines 36-44).

Claim 28

This claim is rejected as applied to the like elements of claim 15 as stated above.

Claim 29

Lee discloses:

The method as claimed in claim 25, wherein said result message is transmitted by said interface to a token device external of said computing entity (col. 3, lines 32-58; col. 6, lines 53-67).

Claim 30

Sprunk discloses:

The method as claimed in claim 25, comprising the step of reporting a result of said monitoring operation by generating a visual display of confirmation data (col. 7, lines 27-37 and col. 8, lines 33-47).

Claim 31

Lee discloses:

The method as claimed in claim 25, further comprising the step of adding a digital signature data to said result message, said digital signature data identifying said

monitoring component; and transmitting said result message and said digital signature data from said interface (col. 7, line 62-col. 8, line 6).

Claim 32

Lee discloses:

A method of obtaining verification of a state of a computer entity, said computer entity comprising a computer platform and a monitoring component (col. 6, lines 53-60), said method comprising the steps of:

an application requesting access to a functionality from a token device (col. 2, lines 27-39);

in response to said request for access to functionality said token device generating a request signal requesting a verification data from said monitoring component (col. 7, lines 17-34);

in response to said request for verification, said monitoring component reporting a result message to said token device (col. 7, lines 17-34).

by receipt of a satisfactory said result message, said token device offers said functionality to said application (col. 8, lines 49-57).

Lee, however, does not expressly disclose that said result message describing a result of a monitoring operation.

Sprunk teaches a technique that by which the integrity of a computing component is checked (corresponding to the recited monitoring operation) by another computing component (corresponding to the recited monitoring component) in order to

find out or describe the status of the first computing component (col. 1, lines 58-62; col. 3, lines 20-25; col. 5, lines 13-20; col. 6, lines 13-22; col. 13, lines 11-19).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Lee by the teaching of Sprunk, because it ensures that the network meets a minimum reliability standard (col. 8, lines 33-47).

Claim 38

Lee discloses:

A method of checking an integrity of operation of a computing entity, said computing entity comprising a computer platform having a first processor means and first data storage means (col. 5, lines 55-67), and a monitoring component comprising a second processor and second memory means (col. 3, lines 43-67, where security module corresponds to the recited monitoring component), by means of a token device, said token device comprising a third data processor and a third memory means (col. 1, lines 8-14), said method comprising the steps of:

programming said token device to respond to a received poll signal from an application program, said poll signal received from said computer platform (col. 6, lines 37-52);

said token device receiving a poll signal from said computer platform (col. 6, lines 37-52);

in response to said received poll signal, said token device generating a signal for requesting a verification operation by said monitoring component (col. 7, lines 17-34); and

Lee, however, does not expressly disclose that said monitoring component performing a verification operation of said computer platform in response to said received signal from said token device.

Sprunk teaches a technique that by which the integrity of a computing component is checked (corresponding to the recited verification operation) by another computing component (corresponding to the recited monitoring component) in order to find out the status of the first computing component (col. 1, lines 58-62; col. 3, lines 20-25; col. 5, lines 13-20; col. 6, lines 13-22; col. 13, lines 11-19).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Lee by the teaching of Sprunk, because it ensures that the network meets a minimum reliability standard (col. 8, lines 33-47).

Claim 42

Lee discloses:

A method of verifying a status of a computing entity, by means of a token device provided external of said computing entity (col. 1, lines 8-14), said method comprising the steps of:

said token device receiving a poll signal (col. 6, lines 37-52);

said token device responding to said poll signal by providing a request for obtaining verification of a state of said computer entity (col. 7, lines 17-34); and

said token device receiving a result message, said result message describing the result of said verification (col. 7, lines 17-34).

Claim 43

Lee discloses:

A method by which a token device can obtain verification of a state of a computing platform (col. 6, lines 53-67),

a monitoring component being capable establishing an identity of itself (col. 7, lines 17-25, where MAC corresponds to the recited identity); and

wherein said token device has data processing capability and behaves in an expected manner (col. 1, lines 8-14; col. 6, lines 53-67; col. 7, lines 17-34);

said token device being physically separable from said computing platform and said monitoring component (Figs. 2 and 4), said token device having cryptographic data processing capability (col. 6, lines 53-67)

wherein, said monitoring component proves its identity to said token device (col. 7, lines 17-34)

Lee, however, does not expressly disclose that said monitoring component being capable of performing at least one data check on said computer platform and establishing a report of said at least one data check performed on said computing platform.

Sprunk teaches a technique that by which the integrity of a computing component is checked (corresponding to the recited performing at least one data check) by another computing component (corresponding to the recited monitoring component) in order to find out or describe the status (corresponding to the recited establishing a report) of the first computing component (col. 1, lines 58-62; col. 3, lines 20-25; col. 5, lines 13-20; col. 6, lines 13-22; col. 13, lines 11-19).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Lee by the teaching of Sprunk, because it ensures that the network meets a minimum reliability standard (col. 8, lines 33-47).

Claim 44

Lee discloses:

A token device comprising a data processor and a memory device (col. 1, lines 8-14), said token device configured to perform at least one data processing or signaling function (col. 1, lines 8-14; col. 6, lines 53-67; col. 7, lines 17-34):

wherein said token device operates to:

receive an integrity check data from an external source (col. 7, lines 17-34);

if said integrity check data supplied to said token device is satisfactory, then said token device allows a said function (col. 7, lines 17-34; col. 8, lines 49-57); and

if said integrity check data received by said token device is unsatisfactory, then said token device denies said function (col. 7, lines 17-34; col. 8, lines 49-57).

Claim 41

This claim is rejected as applied to the like elements of claims 22, 24 and 32 as stated above.

Claims 45-47 and 57

Lee discloses:

A system as claimed in claims 1, 18 and 44, wherein said token device is a smart card (col. 1, lines 15-25).

Claim 55

Lee discloses:

The system as claimed in claim 48, wherein the monitoring component is mounted on a common assembly with the first processor (see Fig. 1 and col. 5, lines 5-12).

Claim 56

Lee in view of Sprunk discloses:

The system as claimed in claim 48, wherein one or more of said data checks comprise a check of the integrity of the basic input/output software for one or more components of the computing apparatus (Lee, col. 5, lines 50-54).

Claim 58

Lee discloses:

The system as claimed in claim 53, wherein the portable user token is a smart card, and the token interface comprises a smart card reader (col. 1, lines 15-25; Fig. 1).

Claim 59

Lee discloses:

A computing entity comprising:

computing platform having a first data processor and a first memory (col. 5, lines 55-67);

a monitoring component having a second data processor and a second memory (col. 3, lines 43-67, where security module corresponds to the recited monitoring component),

a communications interface for communicating with a portable user token (see Fig. 1, 132-136), said communications interface having a communication path to the monitoring component (see Fig. 1),

wherein said computing entity is configured such that said monitoring component is adapted to report said data checks to a portable user token connected to the communications interface,

Lee, however does not disclose that said monitoring component is configured to perform a plurality of data checks on said computing platform, said data checks containing data describing a status of said computing platform.

Sprunk teaches a mechanism that by which the integrity of a computing component is checked (corresponding to the recited a plurality of data checks) by another computing component (corresponding to the recited monitoring component) in order to find out the status of the first computing component (col. 1, lines 58-62; col. 3, lines 20-25; col. 5, lines 13-20; col. 6, lines 13-22; col. 13, lines 11-19). Sprunk further teaches that the verifying component describes the status of the component being verified by determining the trustworthiness of that computing component (col. 3, lines 20-25; col. 6, lines 13-22).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Lee by the teaching of Sprunk, because it ensures that the network meets a minimum reliability standard (col. 8, lines 33-47).

Claim 60

This claim is rejected as applied to the like elements of claim 19 as stated above.

Claim 61

Lee discloses:

A system as claimed in claims 1, 18 and 44, wherein said token device is a smart card (col. 1, lines 15-25).

2. Claims 3-5, 9, 33, 34, 36 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lee (5,923,759) in view of Sprunk (5,822,431) as applied to claims 1 and 2 above, and further in view of Perlman et al (6,230,266 B1, hereinafter Perlman).

Claims 3-5, 9, 33 and 34

Lee in view of Sprunk does not expressly disclose that the system as claimed in claim 1, further comprising a third party server, wherein a response to said integrity challenge is sent to said third party server.

Perlman teaches a system having a server that receives information from a verifying principal (corresponding to the recited token device or monitoring component) to verify the status of a certificate (col., line 56-col. 6, line 1-15).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Lee in view of Sprunk by the teaching of Sprunk, because it would provide a technique to ascertain if a computing element has been compromised (col. 4, lines 22-28).

Claim 36

Lee discloses:

a server sends a simplified integrity response to said token device col. 7, lines 17-34).

Lee in view of Sprunk does not expressly disclose that the system as claimed in claim 32, comprises a third party server.

Perlman teaches a system having a server that receives information from a verifying principal (corresponding to the recited token device or monitoring component) to verify the status of a certificate (col., line 56-col. 6, line 1-15).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Lee in view of Sprunk by the teaching of Sprunk, because it would provide a technique to ascertain if a computing element has been compromised (col. 4, lines 22-28).

Claim 37

Lee in view of Sprunk discloses:

The method as claimed in claim 32, further comprising the steps of:

adding a digital signature data to a simplified integrity response, said digital signature data authenticating a server to said token device (Lee, col. 7, line 62-col. 8, line 6).

Lee in view of Sprunk does not expressly disclose that the system as claimed in claim 32, comprises a third party server.

Perlman teaches a system having a server that receives information from a verifying principal (corresponding to the recited token device or monitoring component) to verify the status of a certificate (col., line 56-col. 6, line 1-15).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Lee in view of Sprunk by the teaching of Sprunk, because it would provide a technique to ascertain if a computing element has been compromised (col. 4, lines 22-28).

Allowable Subject Matter

Claims 6-8 and 35 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132

July 26, 2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100